The Signature Scheme Zalcon An integer-friendly variant of Falcon

Gaël Claudel*[1]

[1]Centre Inria de l'Université de Rennes – Institut National de Recherche en Informatique et en Automatique – France

Résumé

Abstract.
To anticipate the feasibility of quantum computers, in 2017 NIST launched a competition for new post-quantum cryptographic algorithms. As part of this effort, Falcon, a signature scheme, was standardized (along with others such as Dilithium). However, Falcon relies on the use of floating-point numbers, which leads to implementation and security issues. In order to get rid of floating-point arithmetic, a NIST workshop outlined a variant that only handles integers, called Zalcon. This work adds the missing parts, though the design was previously incomplete.

This talk is the sequel to Laz Panard's master's thesis, presented at JC2 2025.
The earlier challenges of making Zalcon running involved algorithmic choices and parameters analysis. Panard's work detailed how to compute the approximate Cholesky decomposition of the perturbation covariance matrix in the cyclotomic integer ring -completing Zalcon's implementable design- and analyzed how this affects the scheme's parameters and assumptions, along with an analysis of the signature procedure's parameters. Panard also presented a working Python proof-of-concept for Zalcon.

This talk will focus on the stand-alone fixed-point implementation in C. We used Thomas Pornin's fixed-point implementation of Falcon key generation as a starting point. Then we made the algorithmic modifications needed (like the Cholesky approximation). Our implementation includes the key generation, the signature, and the verification procedure. We do not use any external libraries to perform the computation (multi-precision, fixed point, modular computations), making the implementation embedded-friendly. This will be the first reference implementation of Zalcon. It may serve as a basis for future work.

Collaboration with: Laz Panard, Pierre-Alain Fouque, Benoît Gérard, Aurore Guillevic, Damien Marion, Daniel De Almeida Braga.

*Intervenant